

Nama: Aga Wira Julyansyah (09011381722099)  
Sistem Komputer 4A

Tugas Komunikasi Data

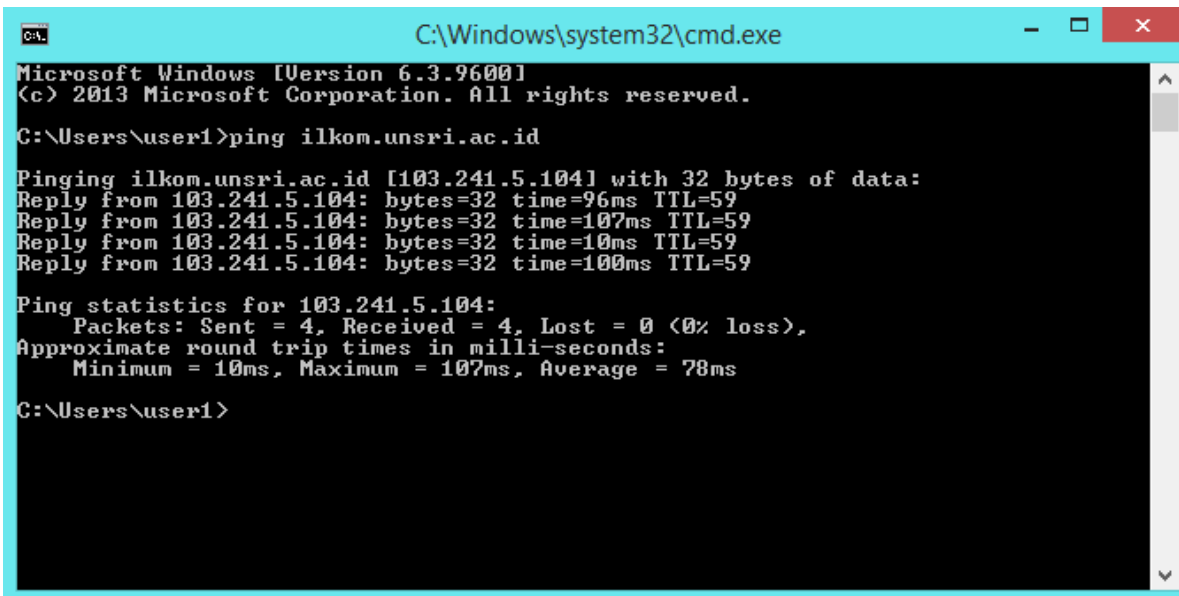
---

## Menganalisis Packets menggunakan Wireshark

Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang Anda kelola. Wireshark menggunakan interface yang menggunakan Graphical User Interface (GUI).

Wireshark mampu menangkap paket-paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa.

Saat ini saya akan menganalisis packet protokol yang ter capture saat membuka situs website (ilkom.unsri.ac.id), sebelum itu kita harus membuka terlebih dahulu buka webnya lalu mengetahui ip dari ilkom.unsri.ac.id di CMD, seperti gambar:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\user1>ping ilkom.unsri.ac.id

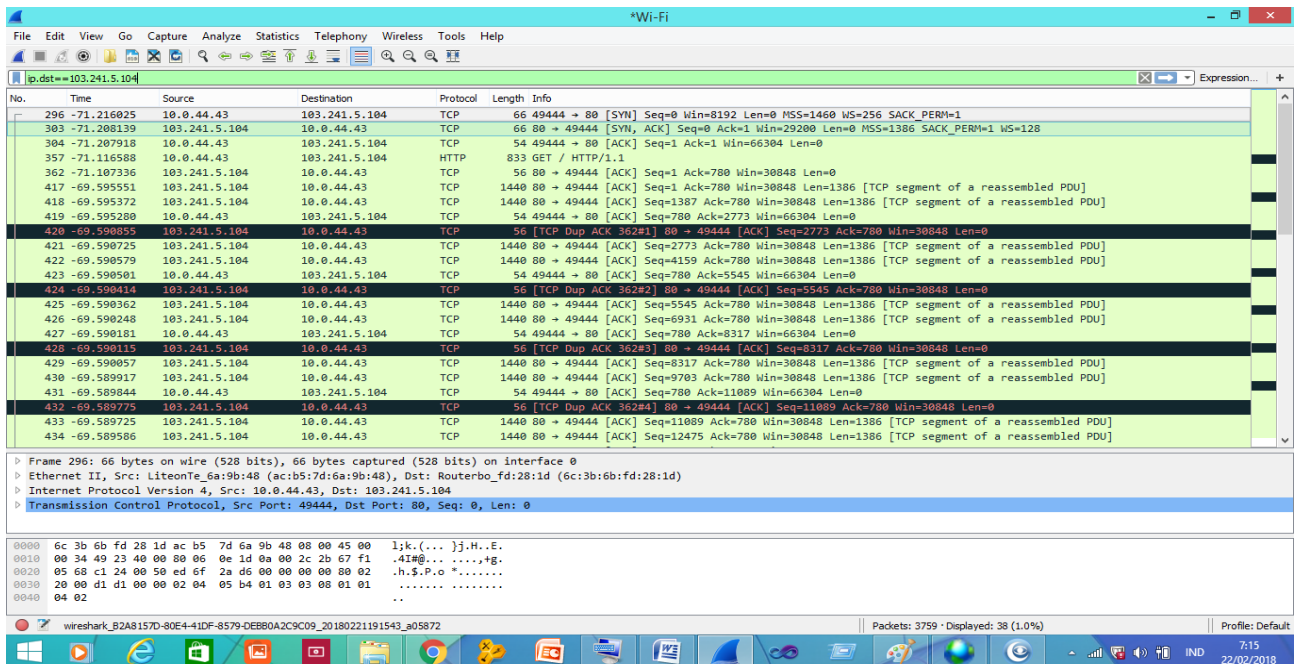
Pinging ilkom.unsri.ac.id [103.241.5.104] with 32 bytes of data:
Reply from 103.241.5.104: bytes=32 time=96ms TTL=59
Reply from 103.241.5.104: bytes=32 time=107ms TTL=59
Reply from 103.241.5.104: bytes=32 time=10ms TTL=59
Reply from 103.241.5.104: bytes=32 time=100ms TTL=59

Ping statistics for 103.241.5.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 107ms, Average = 78ms
C:\Users\user1>
```

saya akan menganalisis packet protokol yang ter capture saat membuka situs website (ilkom.unsri.ac.id).

Setelah itu, buka wireshark lalu meng-capture proses dan klik stop untuk menghentikan capture. Berikut adalah hasil sebagian tampilan yang telah di-capture. Bisa kita lihat pada gambar berikut ini:

berikut hasil analisa jaringan yang ter capture:



Setelah membuka wireshark menekan wifi yang ada pada wireshark maka akan timbul capture saat membuka tab website (ilkom.unsri.ac.id). Saya akan menjelaskan protocol yang tertangkap pada saat membuka (ilkom.unsri.ac.id):

### Menggunakan TCP:

```

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 21 Feb 2018 12:17:16 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: wfvfvt_613827590=5a8d634b19850; expires=Wed, 21-Feb-2018 12:47:15 GMT; Max-Age=1800; path=/; HttpOnly
Referrer-Policy: unsafe-url
x-frame-options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Link: <http://ilkom.unsri.ac.id/wp-json/>; rel="https://api.w.org/"
Content-Encoding: gzip
    
```

Pada baris pertama dapat disimpulkan bahwa versi http yang dipakai ialah /HTTP/1.1, di baris kedua host yang sedang dibuka atau web yang sedang dibuka ialah ilkom.unsri.ac.id, lalu di baris ketiga diketahui bahwa koneksi sedang berjalan atau aktif (keep-alive). Kemudian dibaris kelima browsing menggunakan Mozilla versi 5.0 dan Chrome dan safari. Lalu accept encoding menggunakan format gzip dan deflate. Accept languagenya ialah ID [Indonesia]. Dan pada baris yang menjelaskan cookies artinya sedang berjalan.

Selanjutnya:

```
Wireshark · Follow TCP Stream (tcp.stream eq 10) · wireshark_B2A8157D-80E4-41DF-8579-DEBB0A2C9C09_20180221191543_a05872

GET / HTTP/1.1
Host: ilkom.unsri.ac.id
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: de-DE;q=0.9,en-US;q=0.8,en;q=0.7,id;q=0.6
Cookie: _ga=G41.3.1576985310.1500732161; wordfence_verifiedHuman=f60b28babc9c5e876cd8399bfd592975; _gid=G41.3.612195072.1519211013; _pk_ses.1.da38=*; wfvt_613827590=5a8d625bacd6d; sc_is_visitor_unique=rx10733571.1519215243.94E8A2E918124F784059F42D004CA8135.2.1.1.1.1.1.1.1; _pk_id.1.da38=41700670246698be.1519211013.2.1519215436.1519211067.
```

Pada baris kedua server yang kedua menggunakan server basic ubuntu. Dan waktunya adalah hari Rabu, 21 Februari 2018. Lalu koneksi masih berjalan (keep-alive). Lalu conten encoding menggunakan format gzif.

Selanjutnya:

```
▶ Frame 296: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: LiteonTe_6a:9b:48 (ac:b5:7d:6a:9b:48), Dst: Routerbo_fd:28:1d (6c:3b:6b:fd:28:1d)
▶ Internet Protocol Version 4, Src: 10.0.44.43, Dst: 103.241.5.104
▶ Transmission Control Protocol, Src Port: 49444, Dst Port: 80, Seq: 0, Len: 0

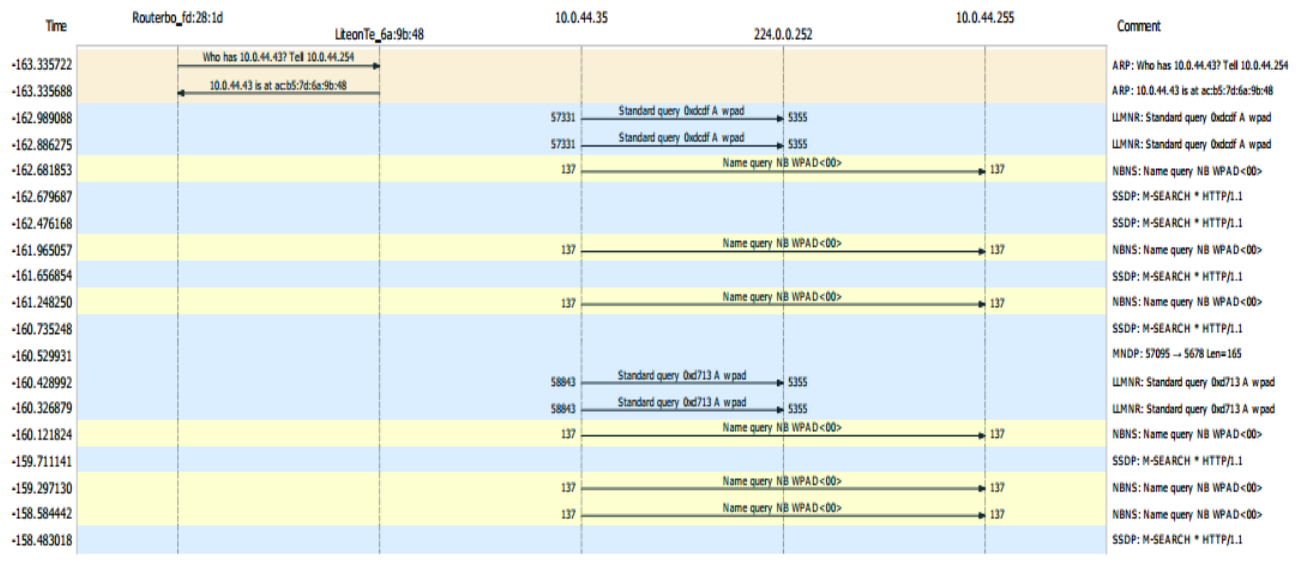
0000  6c 3b 6b fd 28 1d ac b5 7d 6a 9b 48 08 00 45 00  l;k.(... }j.H..E.
0010  00 34 49 23 40 00 80 06 0e 1d 0a 00 2c 2b 67 f1  .4I#@... ..,+g.
0020  05 68 c1 24 00 50 ed 6f 2a d6 00 00 00 80 02  .h$.P.o *.....
0030  20 00 d1 d1 00 00 02 04 05 b4 01 03 03 08 01 01  .....
0040  04 07
```

Pada baris pertama disebutkan frame, frame pada wireshark adalah jaringan (network) 66 bytes on wires dan captured (528 bits) . port 494444, dapat dilihat dari gambar:

```
▶ Frame 440: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
▶ Interface id: 0 (\Device\NPF_{B2A8157D-80E4-41DF-8579-DEBB0A2C9C09})
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 21, 2018 19:17:18.608177000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1519215438.608177000 seconds
    [Time delta from previous captured frame: 0.007370000 seconds]
    [Time delta from previous displayed frame: 0.007370000 seconds]
    [Time since reference or first frame: -69.575280000 seconds]
  Frame Number: 440
  Frame Length: 56 bytes (448 bits)
  Capture Length: 56 bytes (448 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:vssmonitoring]
  [Coloring Rule Name: Bad TCP]
  [Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update]
```

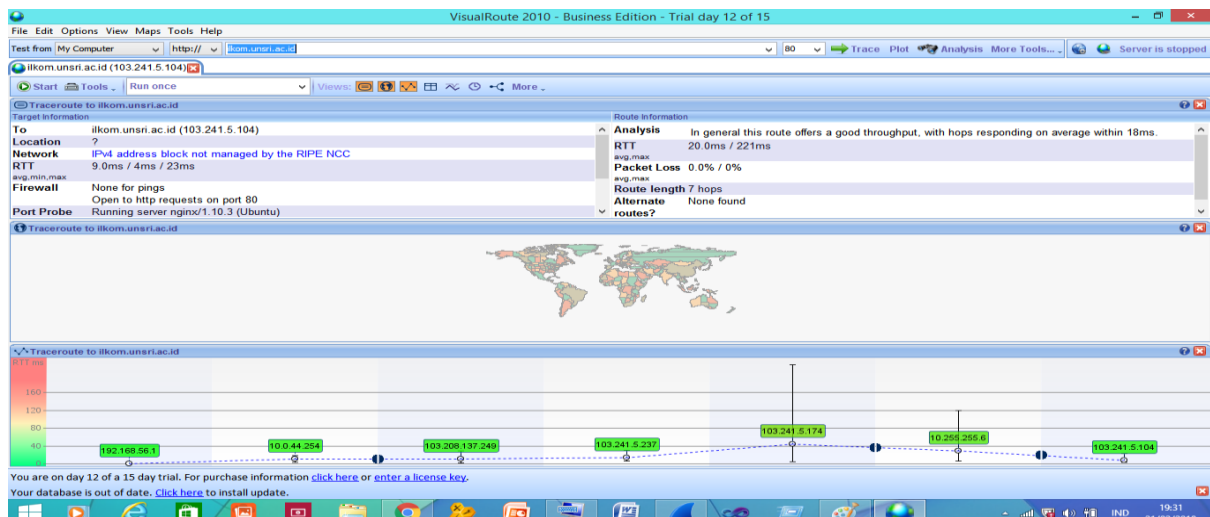
## FLOWGRAPH pada Wireshark (ilkom.unsri.ac.id)

Lihat flow graphnya dengan cara pilih menu statistics>flow graph>klik ok.



Gambar diatas merupakan flow graph dari proses berlangsungnya ssh. Pada flow graph ini kita dapat melihat secara detail bagaimana proses enkripsi tersebut satu per satu. Selain ACK, Pada gambar terdapat encrypted request dan encrypted response . Encrypted request dan encrypted response itu adalah data-data hasil enkripsi yang tidak bisa dilihat oleh sembarang orang.

## Menggunakan Visual Route



## Traceroute to ilkom.unsri.ac.id:

Hops	Loss	IP	Name	Location	Tzone	Avg ms	Min ms	Max ms	Network
0	0	192.168.56.1	user	-	-	0.0	0	0	[Local Network]
1	0	10.0.44.254	-	-	-	11.0	4	19	[Local Network]
2	0	103.208.137.249	ip-103-208-137-249.unsri.ac.id	-	-	12.0	3	29	IPv4 address block not managed by the RIPE NCC
3	0	103.241.5.237	ip-103-241-5-237.unsri.ac.id	-	-	14.0	7	31	IPv4 address block not managed by the RIPE NCC
4	0	103.241.5.174	ilkom-idl.unsri.ac.id	-	-	45.0	5	221	IPv4 address block not managed by the RIPE NCC
5	0	10.255.255.6	-	-	-	29.0	7	120	[Local Network]
6	0	103.241.5.104	ilkom.unsri.ac.id	-	-	9.0	4	23	IPv4 address block not managed by the RIPE NCC

## Diliat dari Colasoft Capsa:

Capsa adalah penganalisa jaringan portabel untuk LAN dan WLAN yang melakukan penangkapan paket secara real-time, memonitoring jaringan, analisis protokol, mendalami paket decoding, dan diagnosis. Ini menyediakan visibilitas yang komprehensif, membantu administrator jaringan atau network engineer agar cepat menentukan dan menyelesaikan masalah berbagai aplikasi, dan karena itu meningkatkan pengalaman pengguna akhir dan menjamin lingkungan jaringan produktif. Capsa adalah alat jaringan yang bagus untuk membantu menurunkan biaya TI, meningkatkan keamanan jaringan, meningkatkan layanan pelanggan, dan lebih lincah

